



Classical Equipment & New Technologies



Dragos Titescu
Systems Engineer

Agenda

- IPS 7.0 with Global Correlation
- ASA with Botnet Traffic Filter
- Q&A
- Security Intelligence Operations

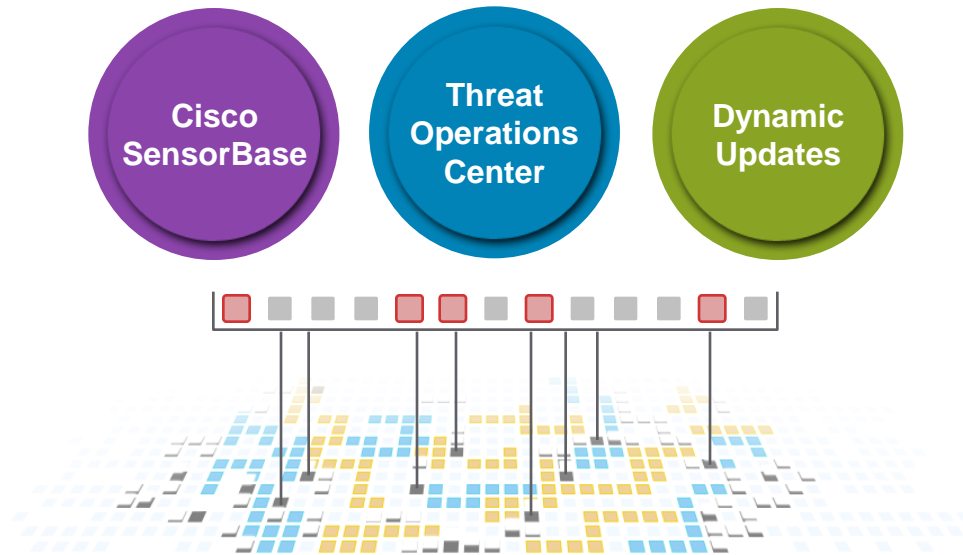




IPS 7.0 with Global Correlation



Cisco Security Intelligence Operations



→ Security Infrastructure That Dynamically Protect Against the Latest Threats Through: ←

Cisco SensorBase

The Most Comprehensive
Vulnerability and Sender
Reputation Database

Threat Operations Center

A Global Team of Security
Researchers, Analysts,
and Signature Developers

Dynamic Updates

Dynamic Updates and
Actionable Intelligence

Powered by Global Correlation

Cisco Global Correlation

SensorBase: World's Largest Traffic Monitoring Network

LARGEST FOOTPRINT

| GREATEST BREADTH |

FULL CONTEXT ANALYSIS



Cisco SensorBase

700,000+ sensors deployed globally

8 of the top 10 global ISPs

Over 500GB of data per day

500 third party feeds

Over 30% of the world's email traffic

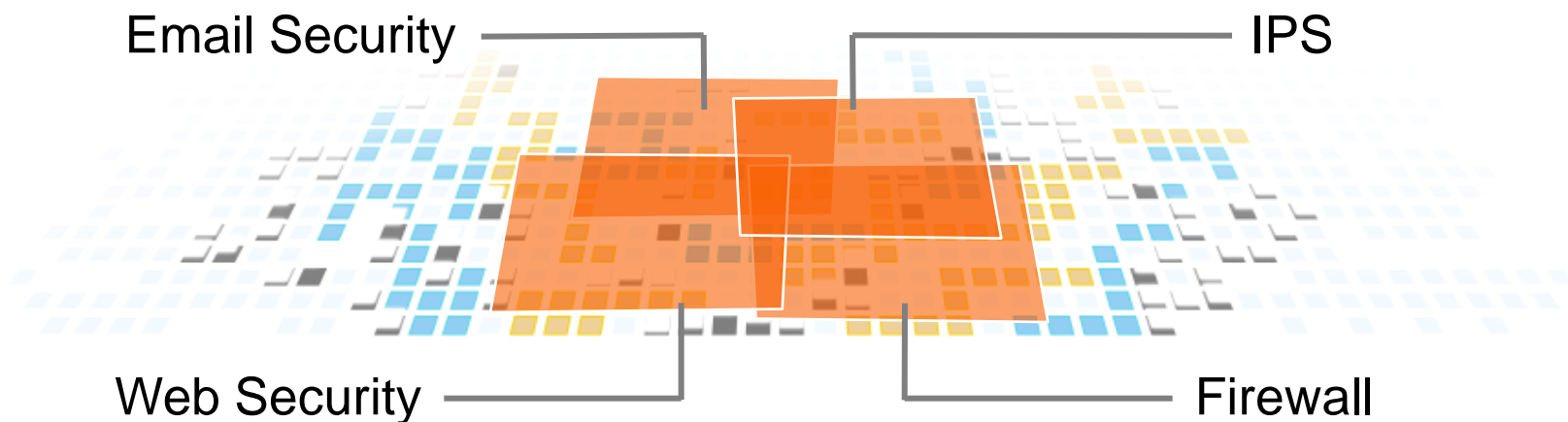
Cisco Global Correlation

Unmatched Breadth

LARGEST FOOTPRINT

GREATEST BREADTH

FULL CONTEXT ANALYSIS



Identifying a global botnet requires complete visibility across all threat vectors

Global Correlation

Full Context Analysis: Seeing the Whole Picture

LARGEST FOOTPRINT

| GREATEST BREADTH

| **FULL CONTEXT ANALYSIS**

What?

Content

Who?

How?

Where?

Global Correlation

Full Context Analysis: Seeing the Whole Picture

LARGEST FOOTPRINT | GREATEST BREADTH | **FULL CONTEXT ANALYSIS**

What?

Content

Who?

Reputation of Counterparty

How?

Propagation & Mutation Methods

Where?

Geographic & Vertical Trends

Defeating SQL Injection

The Challenge of Traditional Signature-Based IPS

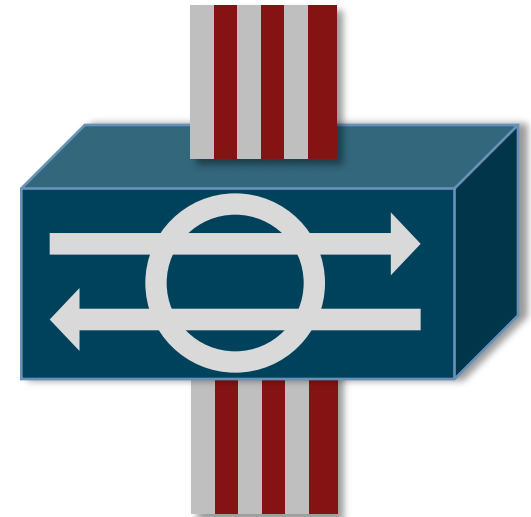
What SIGNATURES Find

Verdict: **UNKNOWN**

What?

SQL Command Fragments
in Web Traffic

This could be your billing system
talking to your customer database.
Or.....



Defeating SQL Injection

Collaborate with Confidence

**What GLOBAL
CORRELATION Knows:**

Verdict: BLOCK

What?

SQL Command Fragments
in Web Traffic from Untrusted Client

Who?

Dynamic IP Address
Dynamic DNS
History of Web Attacks

How?

4th Packet of HTTP Connection

Where?

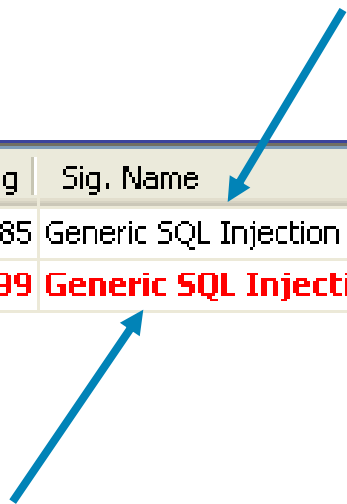
Within Heavily Compromised
Network
History of Botnet Activity



Defeating SQL Injection

Collaborate with Confidence

Traditional Signature only IPS view without Reputation



Risk Rating	Sig. Name	Actions Taken	Attacker IP
85	Generic SQL Injection		30.30.181.133
99	Generic SQL Injection	droppedPacket, deniedFlow, tcpOneWayResetSent	10.20.5.178

Global Correlation Enabled IPS allows Confident Deny Action

IRC Connections

The Challenge of Traditional Signature-Based IPS

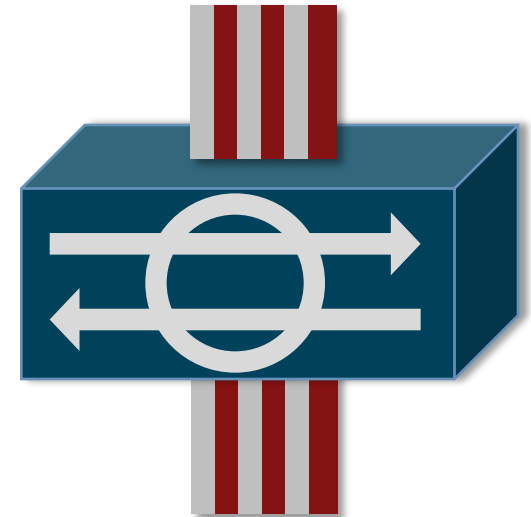
What SIGNATURES Find

Verdict: **UNKNOWN**

What?

IRC Join

This looks like a typical IRC connection request.....



IRC Connections

Collaborate with Confidence

**What GLOBAL
CORRELATION Knows:**

Verdict: BLOCK

What?

IRC Join to Known Botnet Command
and Control Server

Who?

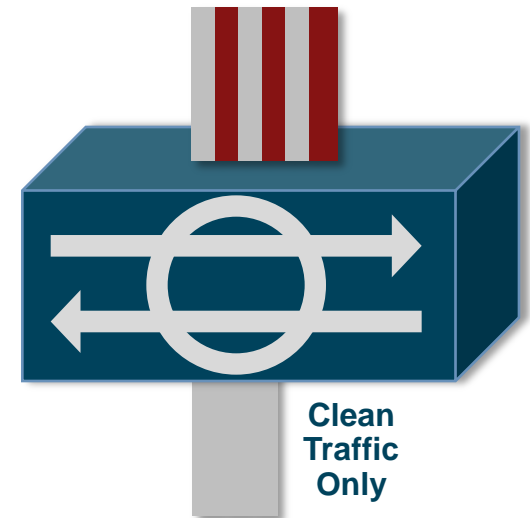
Fast Flux DNS
History of Spam Activities

How?

Standard IRC connection
over known ports

Where?


Within Heavily Compromised
Network
History of Botnet Activity



IRC Connections

Collaborate with Confidence

Traditional Signature only IPS view without Reputation



Risk Rating	Sig. Name	Actions Taken	Attacker IP
73	IRC Channel Join Server Activity		20.20.20.252
96	IRC Channel Join Server Activity	droppedPacket, deniedFlow, tcpOneWayResetSent	10.20.5.59

Global Correlation Enabled IPS allows Confident Deny Action

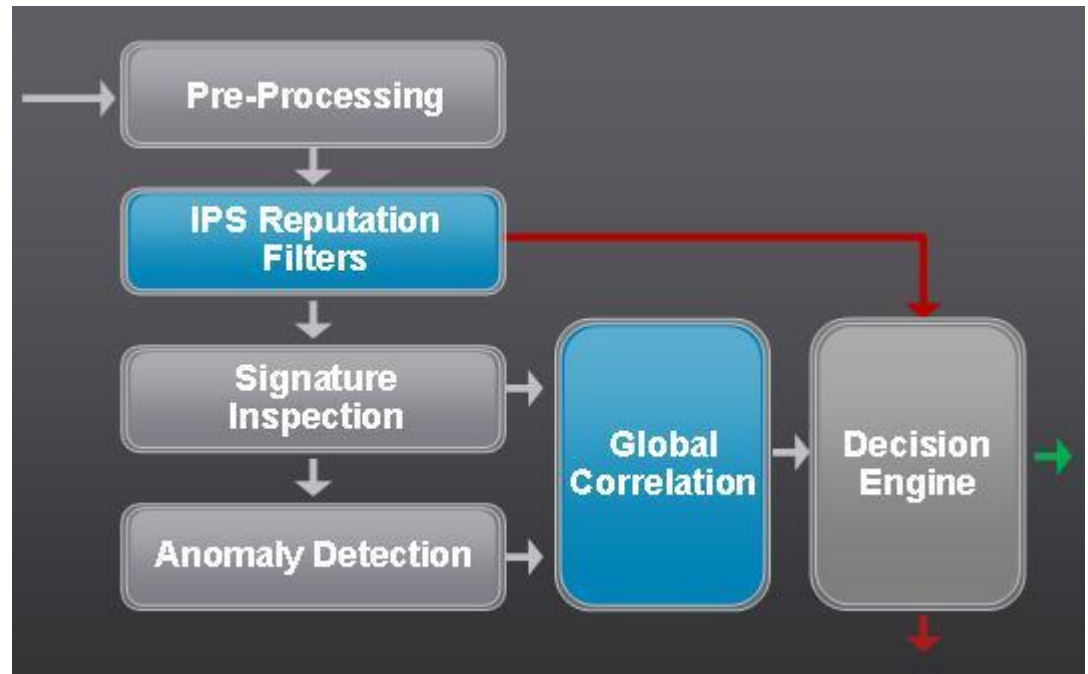


Global Correlation in Detail



Packet Flow in IPS v7.0

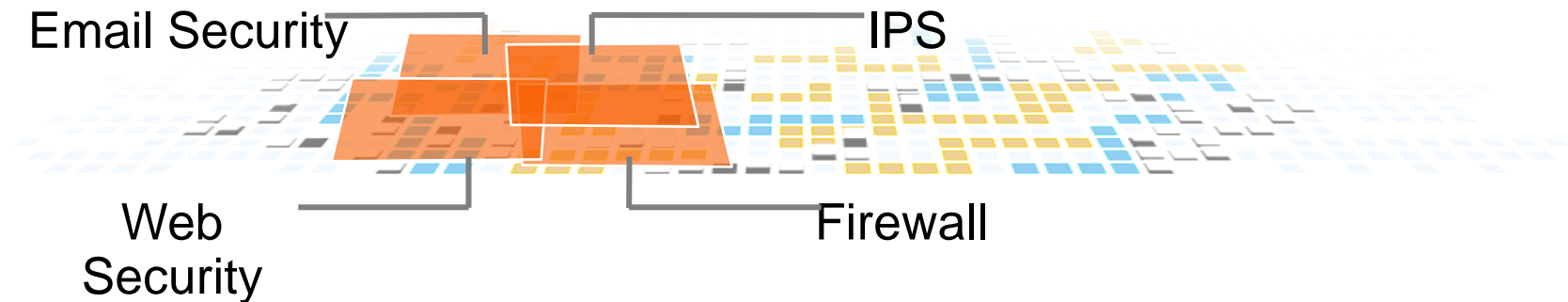
- IPS Reputation Filters block access to IP's on stolen 'zombie' networks or networks controlled entirely by malicious organizations.



- Global Correlation Inspection raises the Risk Rating of events when the attacker has a negative reputation allowing those events to be blocked more confidently and more often than an event without negative reputation.

What is Reputation?

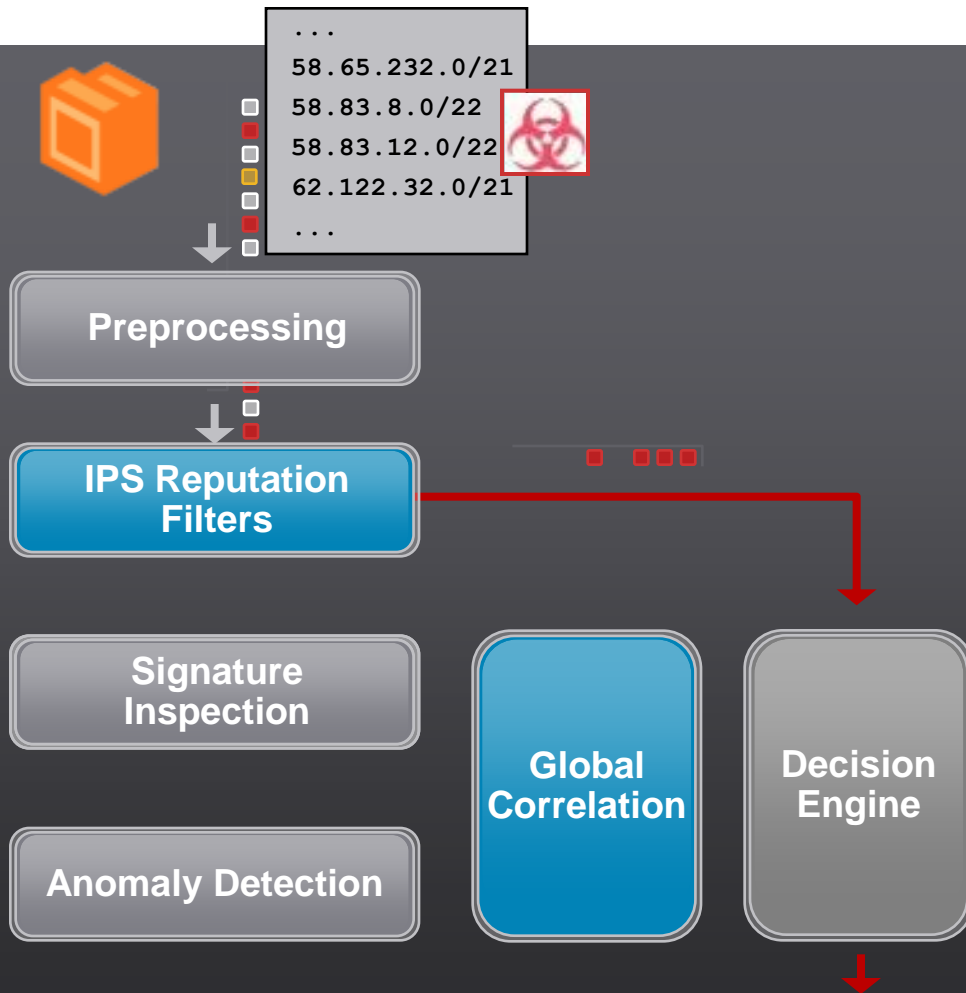
or “Is all reputation the same?”



- Reputation is the history of both actions and qualities of a specific IP address or network. This is calculated using some of the hundreds of different types of data found in Sensorbase.
- For different types of devices, different parameters can mean more or less for the reputation of a device.

Ex: The fact of sending SPAM is highly relevant to an email reputation device and less so to an IPS sensor.

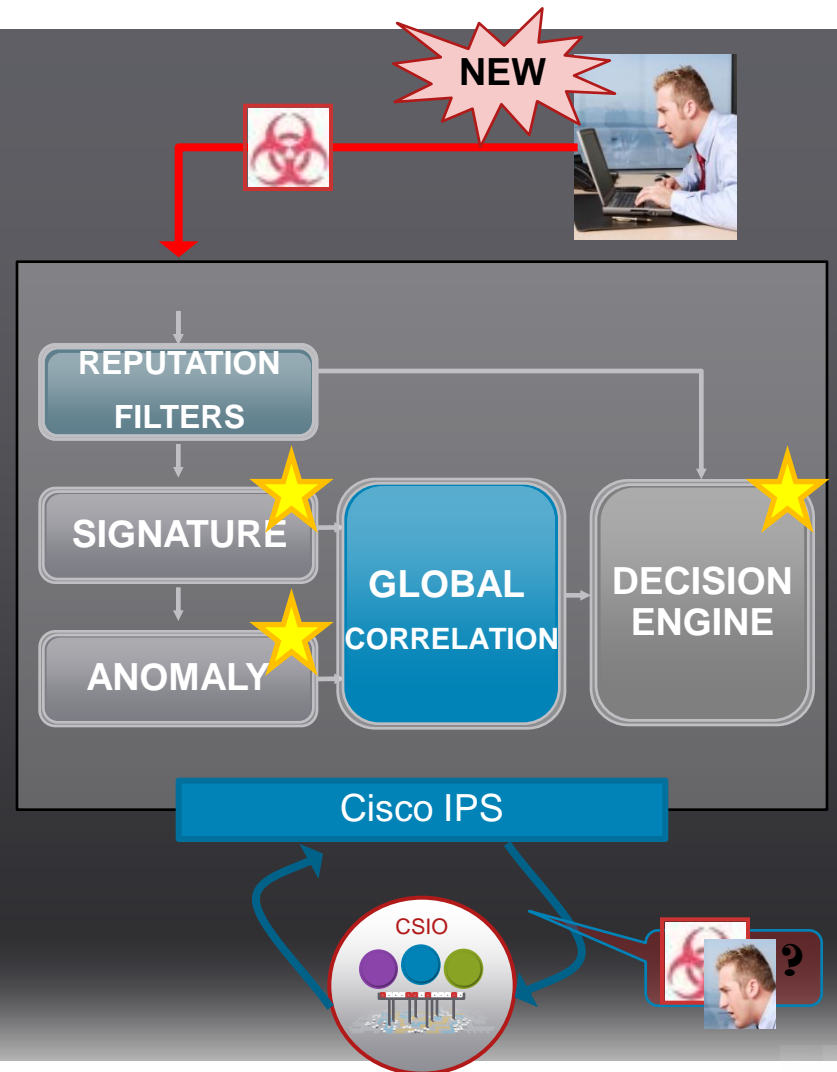
IPS Reputation Filters: Blocking the worst bad apples



- Some networks on the Internet are owned wholly by malicious organizations or are hijacked 'zombie' networks
- Reputation Filters block access to these networks like an ACL
- Individual IP addresses do not go on this list because of things they do (An IP does not go from -1 to -9 to being put on this list)

Local Inspection will Always Matter

Example 1: Unknown Attacker

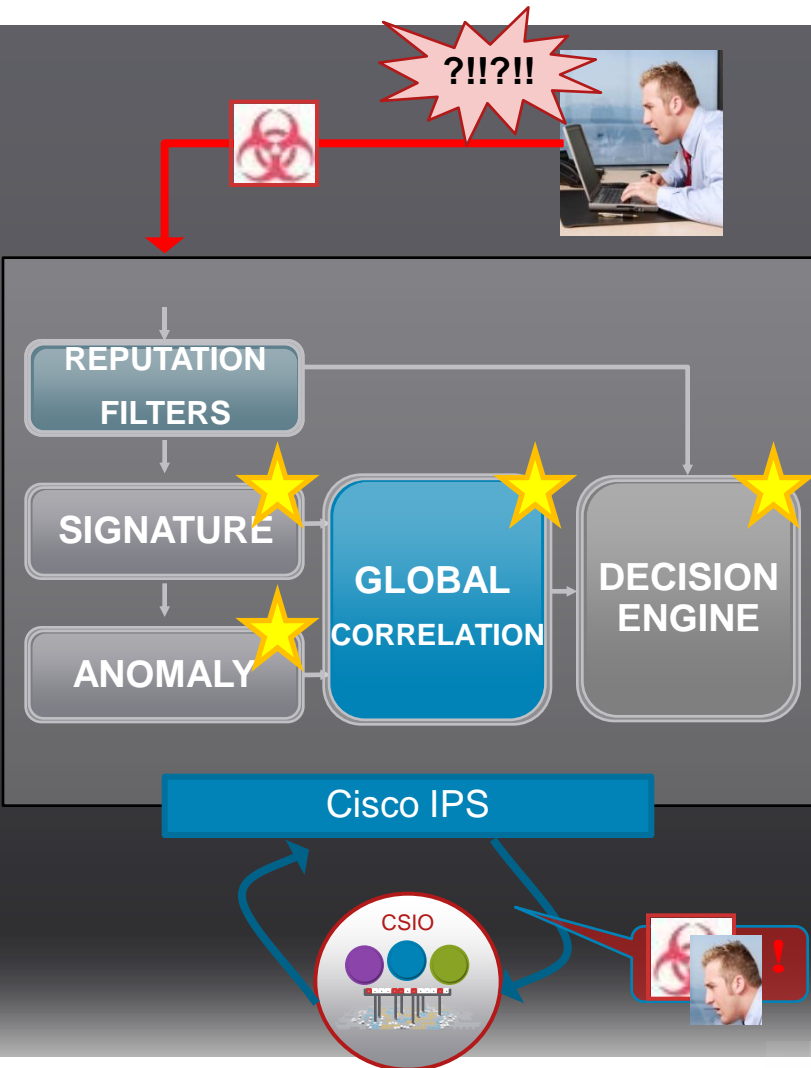


1. New Attacker hits the IPS
2. Attacker without a Reputation
3. Signatures or Anomaly Detection identify activity
4. The attack is handled according to the security policy implemented on the sensor (Deny if Risk Rating reaches threshold)
5. Information on the Attacker is sent back to CSIO to track his reputation (if configured)

Global Correlation Inspection

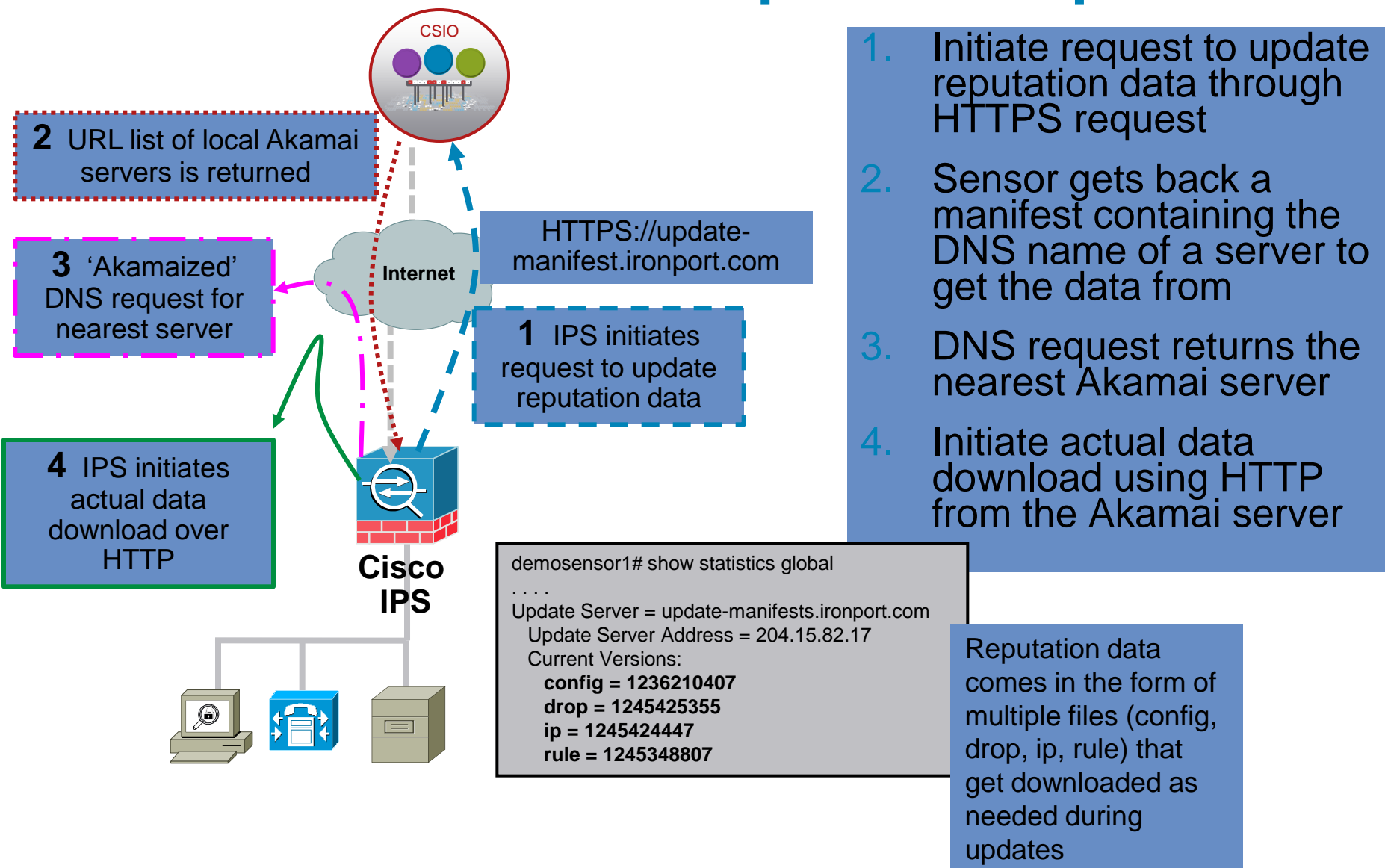
Example 2: Suspicious Attacker

Identified through Local Inspection, Denied due to Global Correlation

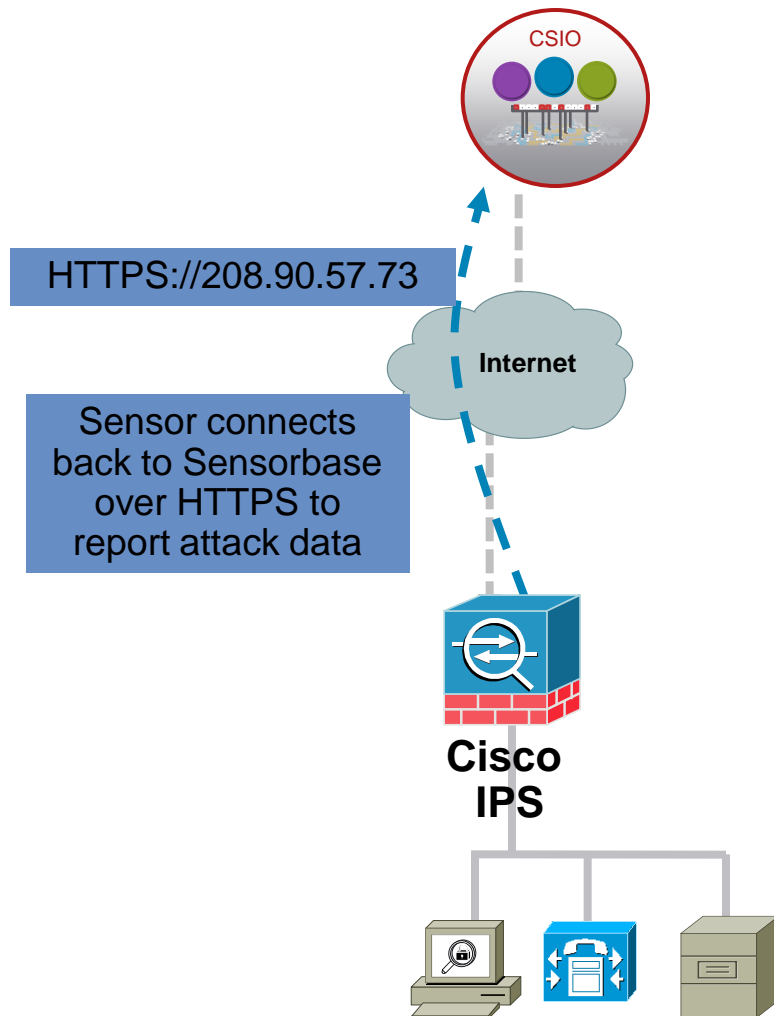


1. Suspicious Attacker attacks
2. Has medium Reputation
3. Signatures identify suspicious activity and give this a medium Risk Rating
4. Global Correlation adds context of Attacker Reputation to Risk Rating
5. Decision Engine blocks
6. Information on NEW Reputation is sent back to CSIO.

Global Correlation Reputation Updates



Global Correlation Network Participation: or “My sensor is sending data back to Cisco?”



- Event data parsed down into Reputation update data on the sensor and buffered for transmission to Cisco Sensorbase
- Every ten minutes on average, network participation data is sent to Cisco over HTTPS
- This data does not include private addresses
- Network Participation improves overall security as well as your own by feeding in attackers data specific to your site.

Global Correlation Network Participation: or “What is my sensor sending back to Cisco?”

Network Participation

Select the extent to which the sensor will contribute data to the SensorBase network.

- ☒ Off Do not contribute data to the SensorBase network.
- ☐ Partial Contribute data to the SensorBase network but withhold some potentially sensitive information.
- ☐ Full Contribute all alert data to the SensorBase network.

Network Participation Disclaimer

If you agree to participate in the SensorBase Network, Cisco will collect aggregated statistics about traffic sent to your IPS. This includes summary data on the Cisco IPS network traffic properties and how this traffic was handled by the Cisco appliances. We do not collect the data content of traffic or other confidential business or personal information. All data is aggregated and sent via secure HTTP to the Cisco SensorBase Network servers in periodic intervals. All data shared with Cisco will be anonymous and treated as strictly confidential.

The table below describes how the data will be used by Cisco.

Participation Level	Type of Data	Purpose
Partial	Protocol Attributes (e.g. TCP max, segment size and options string)	Track potential threats and understand threat exposure
	Attack Type (e.g. Signature Fired and Risk Rating)	Used to understand current attacks and attack severity
	Connecting IP Address and port	Identifies attack source
	Summary IPS performance (CPU utilization memory usage, inline vs. promiscuous, etc)	Tracks product efficacy
Full	Victim IP address and port	Detect threat behavioral patterns

Agree

Disagree

- Network Participation is entirely voluntary and on an Opt-In basis (off by default)
- No actual packet content data is ever sent back
- Partial participation sends back Attacker IP, port, Sig ID and Risk Rating, some protocol attributes and summary IPS performance data
- Full mode adds in Victim IP and port
- Private IP addresses are removed before sending



ASA with Botnet Traffic Filter

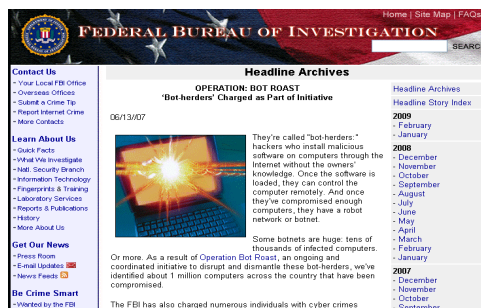


Botnet Epidemic

Overview

- Botnets = network of compromised computers
- 1 to 5 million hosts are believed to have been compromised in the United States and are now being controlled by botnets*

“Operation BotRoast” —FBI

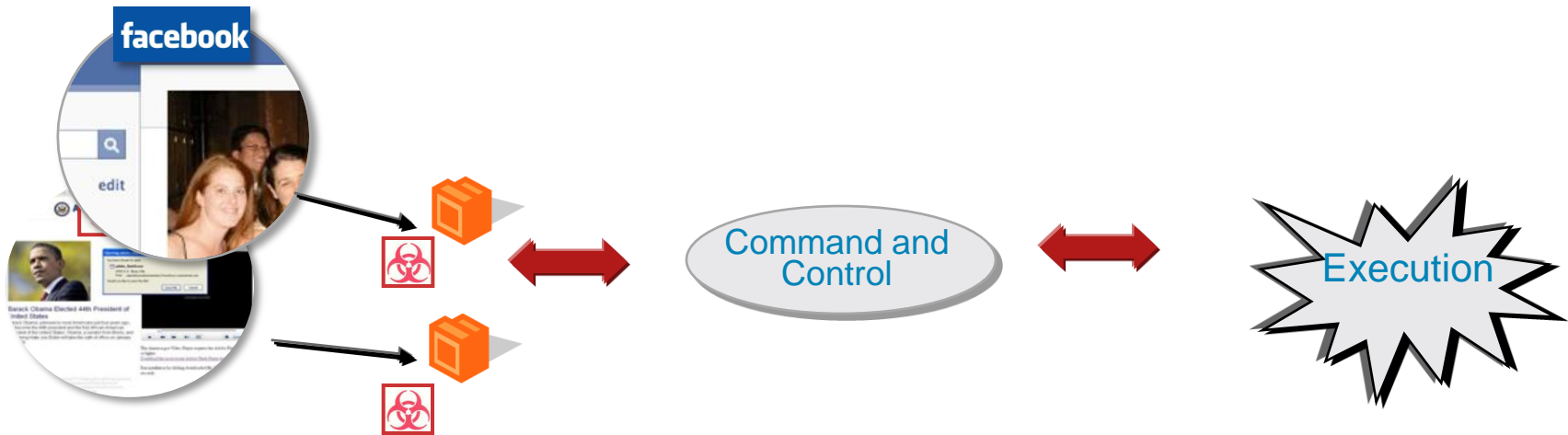


“How Close Is World War 3.0?” —Network World

Attack Profile

- Evolved from spam and denial-of-service attacks to attacks on websites for profit and to take down rival networks
- Profit from attacking a gambling website = US\$50,000

Botnet Infection Process



Step 1:

Clients are infected by spyware, malware, and targeted attacks propagated by web and email

Step 2:

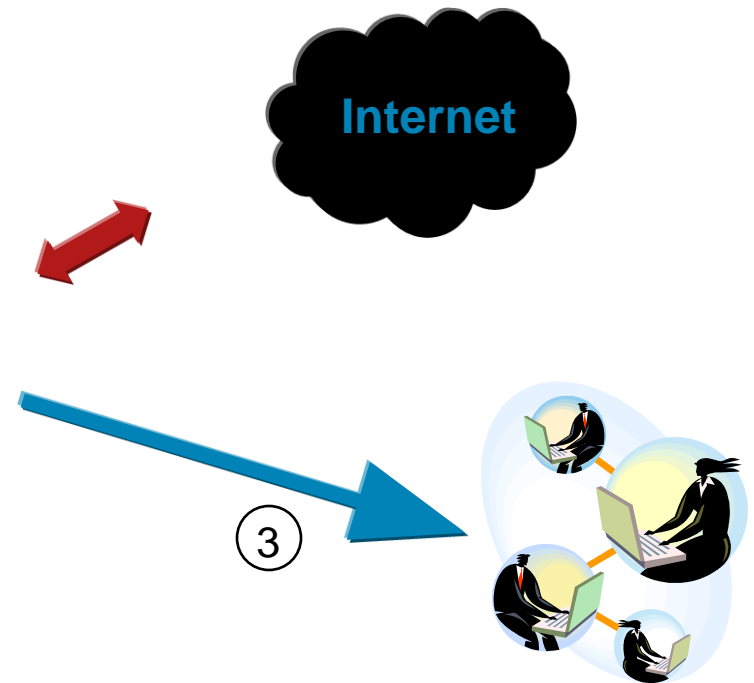
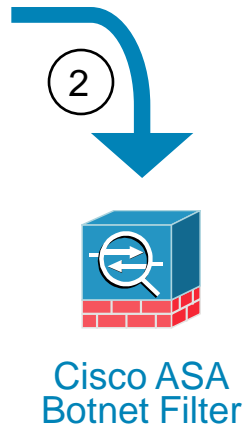
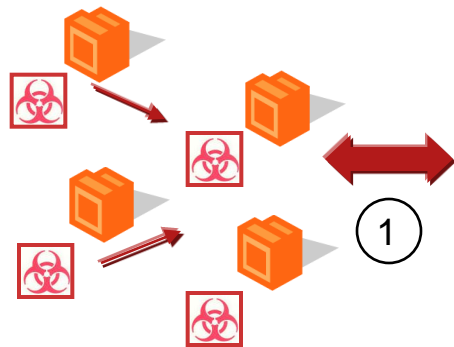
Infected clients communicate with a command and control host on the Internet

Step 3:

Attacks are launched: DoS, ID theft, spam, and click fraud

Botnet Filtering Process

Cisco® Security Intelligence Operations (SIO)



Step 1:

Infected clients try to communicate with a command and control host on the Internet

Step 2:

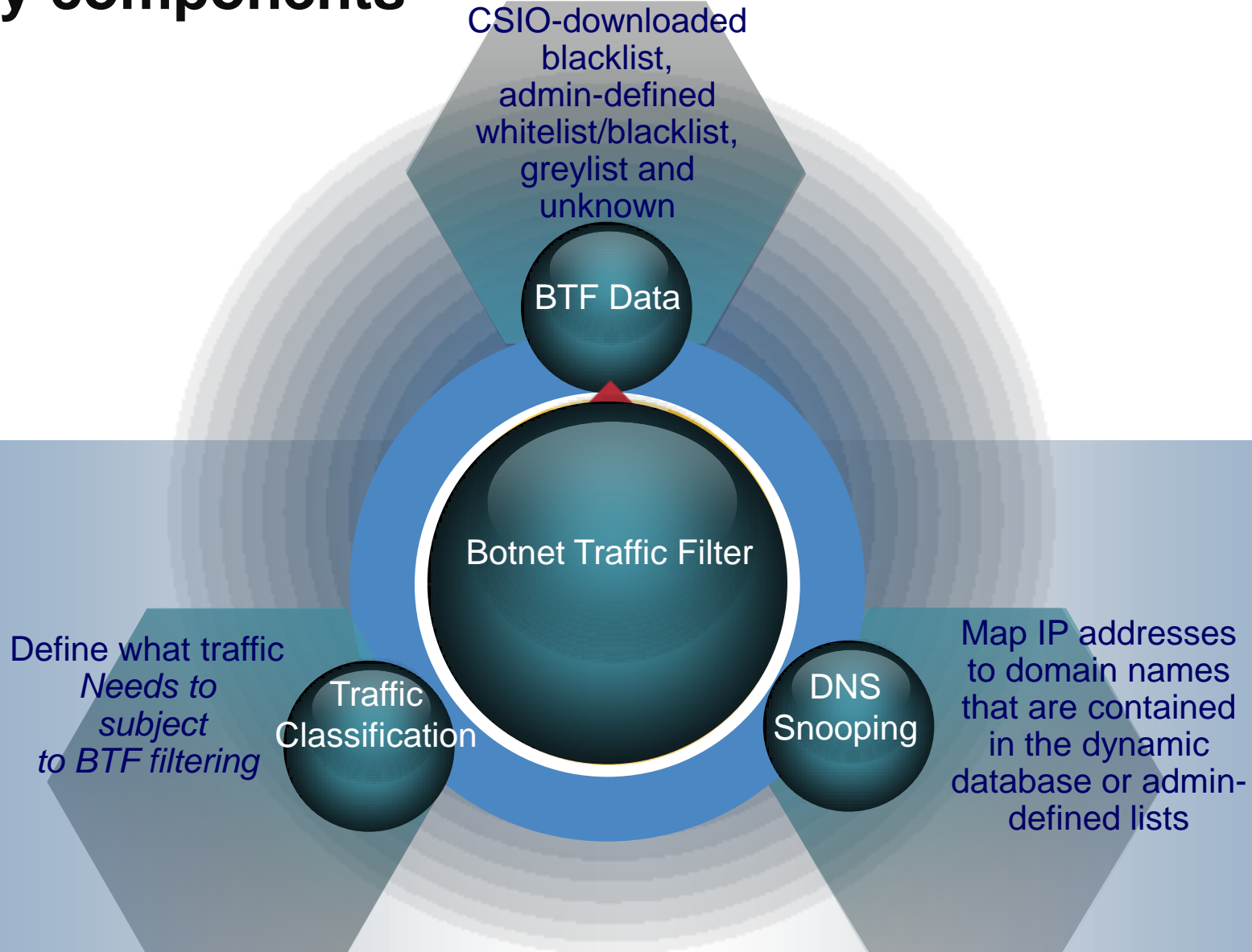
Cisco SIO updates the Cisco ASA botnet filter list; the destination is a known attack site

Step 3:

Alerts go out to the security teams for prevention, mitigation, and remediation

Botnet Traffic Filter

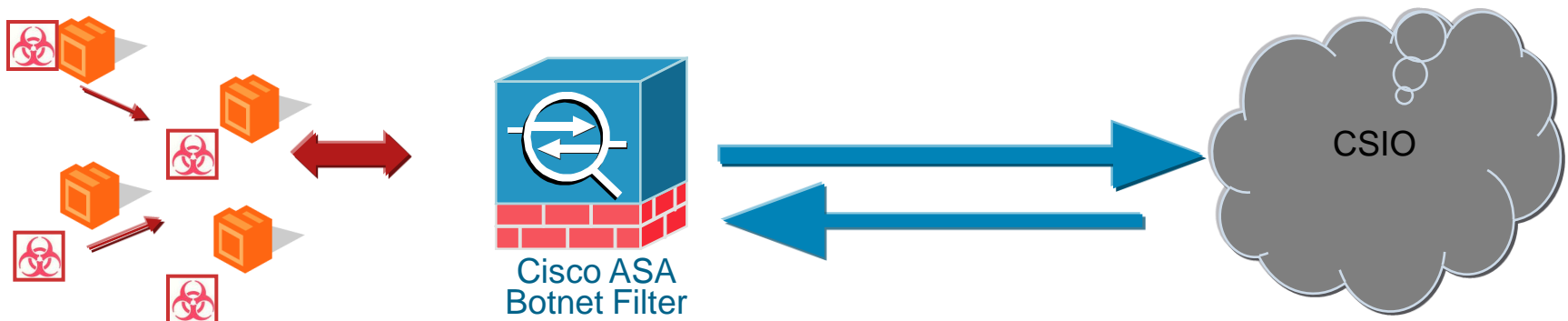
Key components



Botnet Traffic Filter

Database Update Steps

1. Enables BTF update client
2. Waits for 2 minutes before attempting the initial download
3. Contacts updater server at <https://update-manifests.ironport.com>, Initial DB is downloaded
4. Sets the new poll-time
5. Attempts to download new updates at 60-minute interval
6. Update and validate new data and loaded into memory if new update exists.



Botnet Traffic Filter

Traffic Classification

Classify traffic subject to BTF

- Enable specific networks, interfaces or traffic to BTF filtering
- Normally enable on Internet-facing interface

BTF Data Categories

- Blacklist: Known malware sites
- Whitelist: Known allowed addresses
- Greylist: Ambiguous addresses
- Unknown: Unknown and not in any list

BTF Data Types

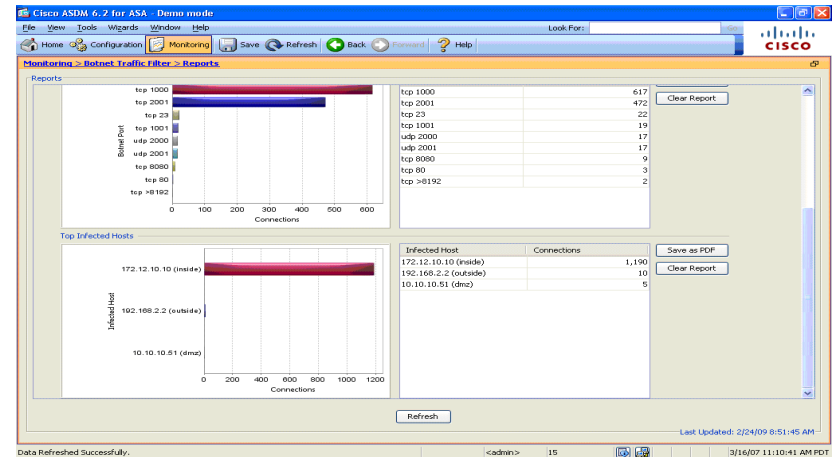
- Dynamic : Data downloaded from CSIO
- Static: Data Defined by security administrators

Note: BTF database does not contain reputation attributes

Botnet Traffic Filter Reporting

- Syslogs (id 338xxx) are generated for dynamic-filter events
- Top 10 infected hosts, sites and ports can be viewed through CLI and ASDM
- Top 10 Reports are independent, not correlated
- Top Reports based on highest hits per category

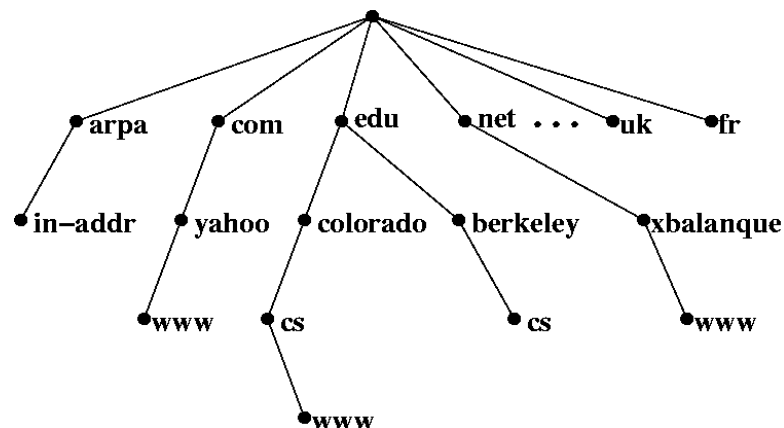
ASA-4-338002: Dynamic Filter permitted black listed TCP traffic from inside:10.1.1.45/6798 (120.160.201.1/7890) to outside:209.165.202.129/80 (209.165.202.129/80), destination 209.165.202.129 resolved from dynamic list: bad.example.com



Botnet Traffic Filter

DNS Snooping

- Watches UDP DNS replies through ASA
- Builds a DNS reverse cache (DNSRC)
- DNSRC housekeeping at 20-minute interval (configurable)
- Life of a DNSRC entry depends on the TTL value in the snooped DNS reply.
- DNSRC size depends on platform.



ASA Model	Maximum DNS reverse cache entries
5505	5,000
5510	10,000
5520	20,000
5540	40,000
5550	40,000
5580	100,000

Botnet Traffic Filter

Deployment Guidelines and Caveats

- Typically deployed on ASA at Internet Edge
- Supported in all modes: single, multiple-context, transparent and routed mode.
- There is about 5-10% performance degradation (largely dependent on DNSRC size)
- Failover:
 - Supported in A/S and A/A
 - DNSRC entries and dynamic DB are not replicated
 - Each ASA in failover pair needs direct connection to update server (<https://update-manifests.ironport.com>)
- Only UDP-based DNS is supported with DNS snooping
- Only IPv4 addresses are supported
- Maximum of 1000 static blacklist and whitelist entries each are supported

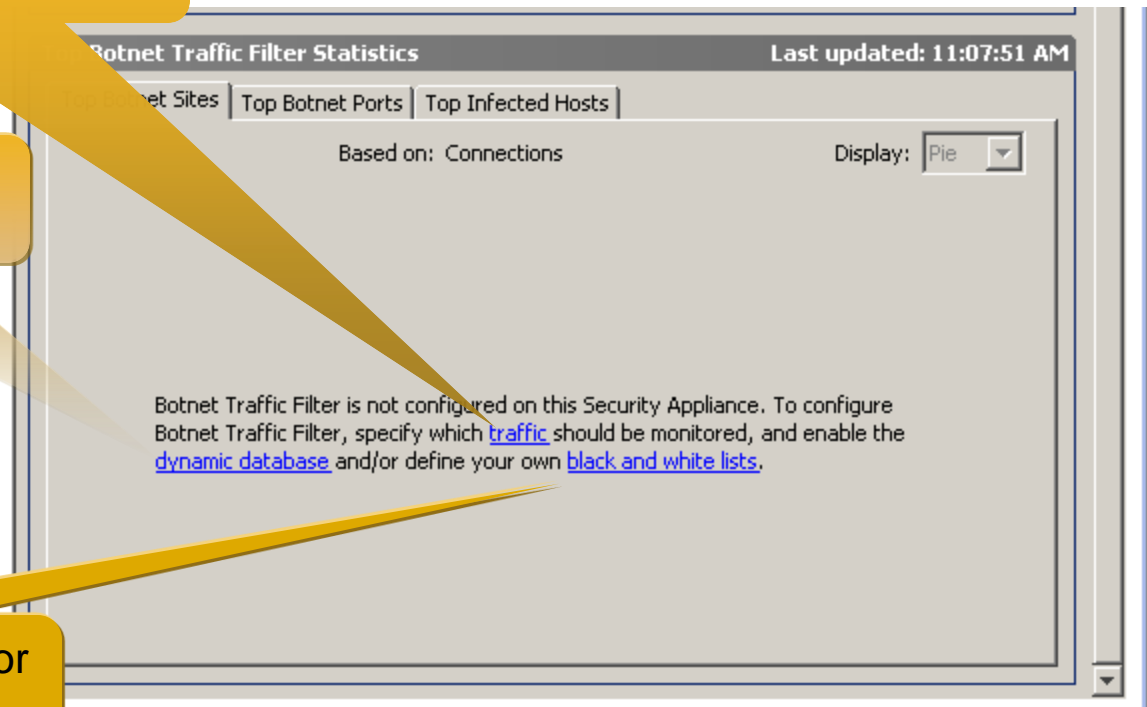
Botnet Traffic Filter

Easy Configuration with Links from the Cisco Adaptive Security Device Manager (ASDM) Dashboard

Select either a global setting or a per-interface setting

Enable download of Cisco® SIO reputation data

Generate the exception lists for your site



Botnet Traffic Filter

Or Enable Directly from Cisco ASDM Configuration Menus

Cisco® SIO

Custom lists

Interface or global

Configuration > Firewall > Botnet Traffic Filter > Botnet Database

Dynamic Database Update

Enabling the Botnet updater client will fetch the latest database from Cisco update server. After the initial fetch, the ASA

☐ Enable Botnet Updater Client

Dynamic Database Configuration

☐ Use Botnet data dynamically downloaded from updater server

Dynamic Database Management

The database can be fetched at anytime. This will not affect the local database maintained in the administrator's lists.

Fetch Botnet Database

The database can be purged at anytime. This will not affect the local database maintained in the administrator's lists.

Purge Botnet Database

Search Dynamic Database

The search will return a single exact match or up to two partial matches, if any.

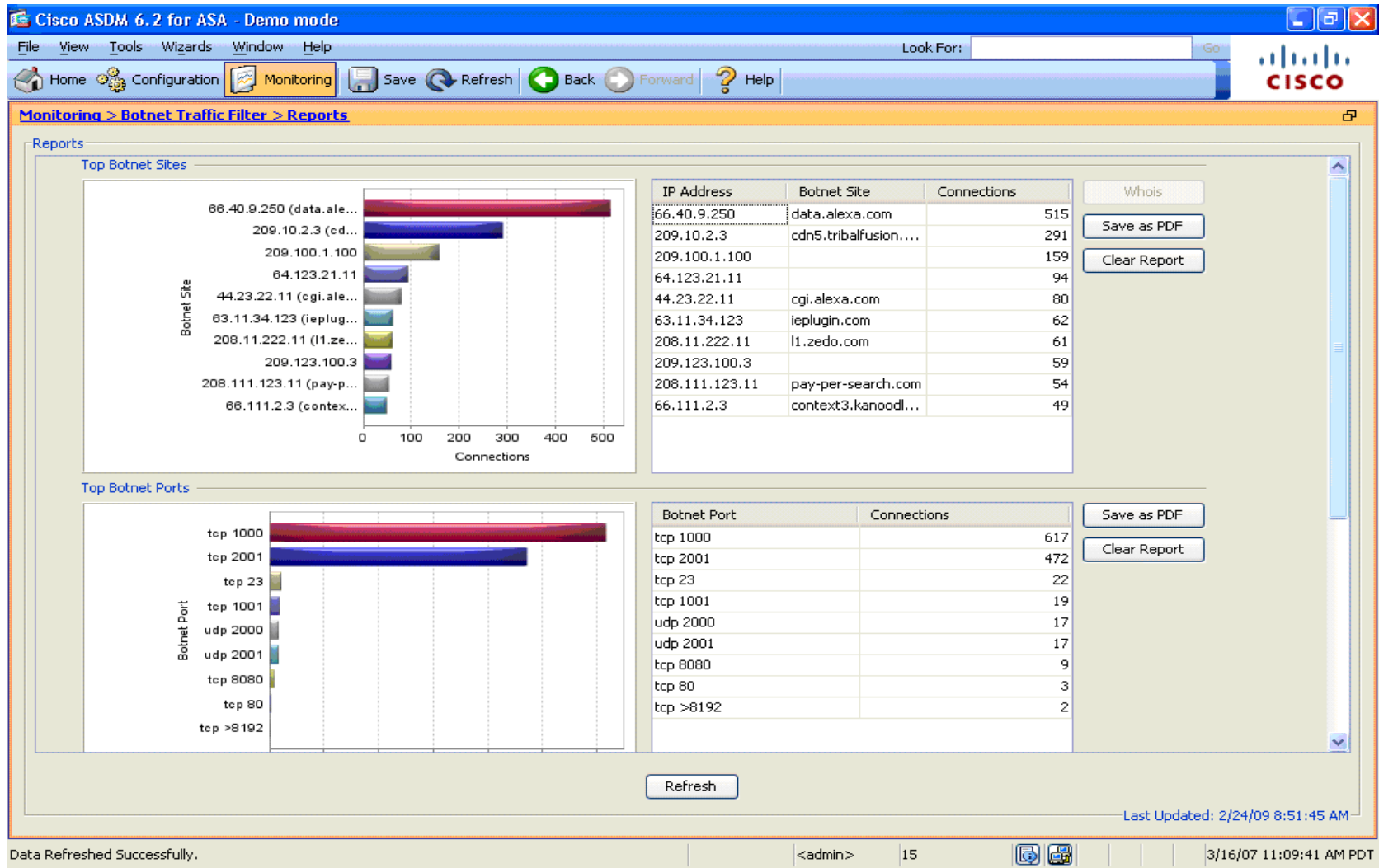
Search for:

Find Now

Clear

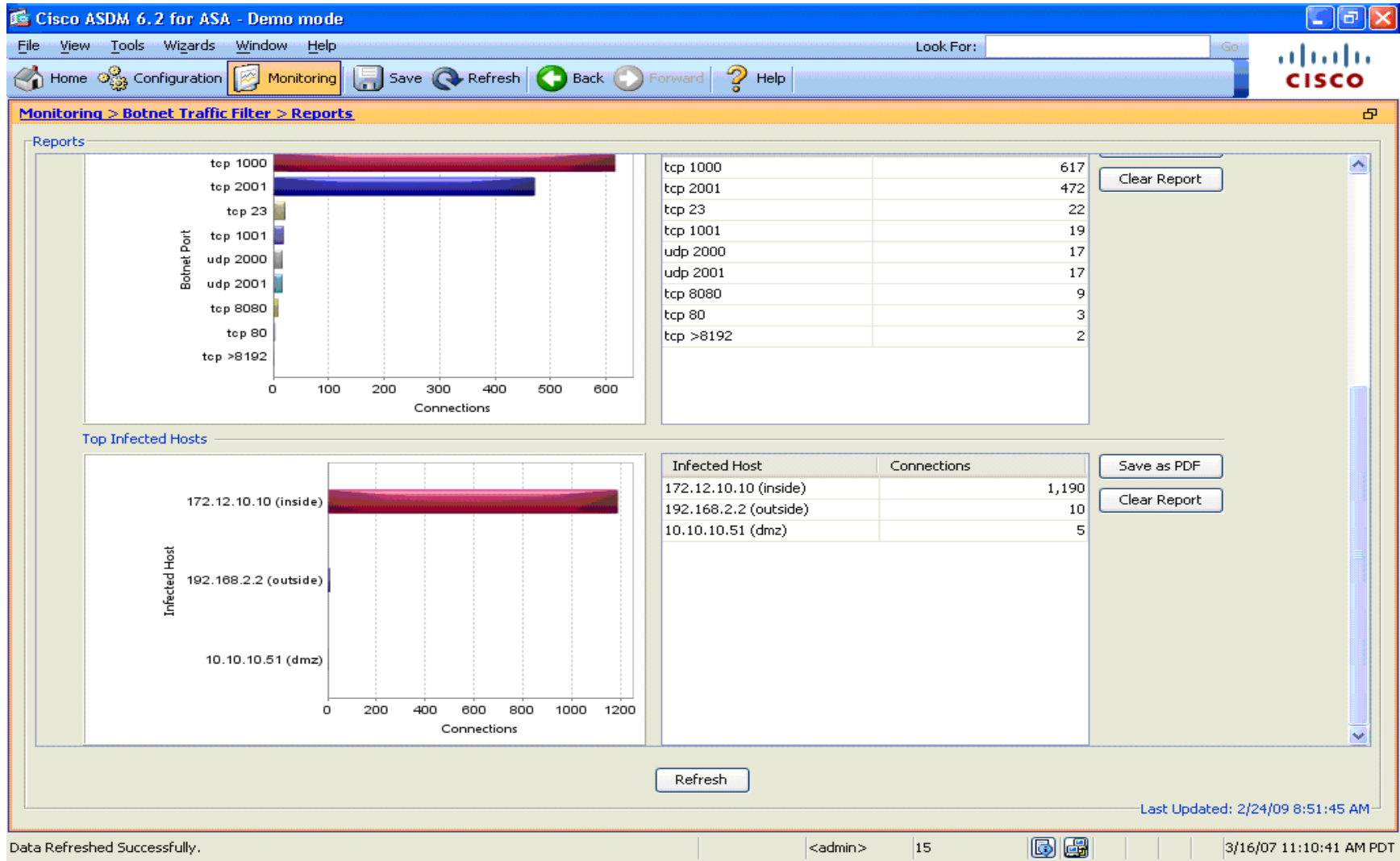
Botnet Traffic Filter Reports

Top Botnet Sites and Ports



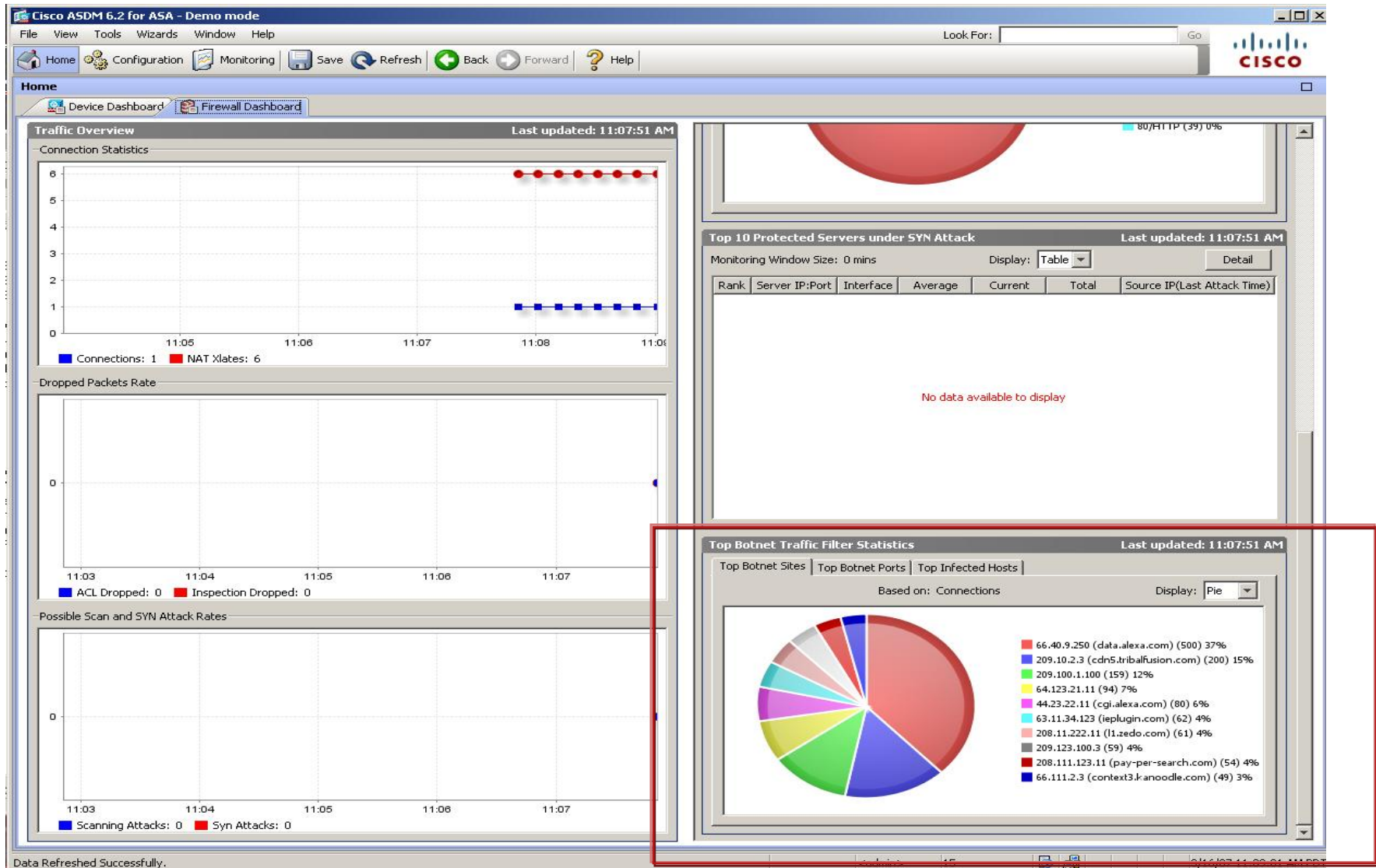
Botnet Traffic Filter Reports

Top Infected Hosts



Cisco ASDM Dashboard

Botnet Traffic Filter Integration





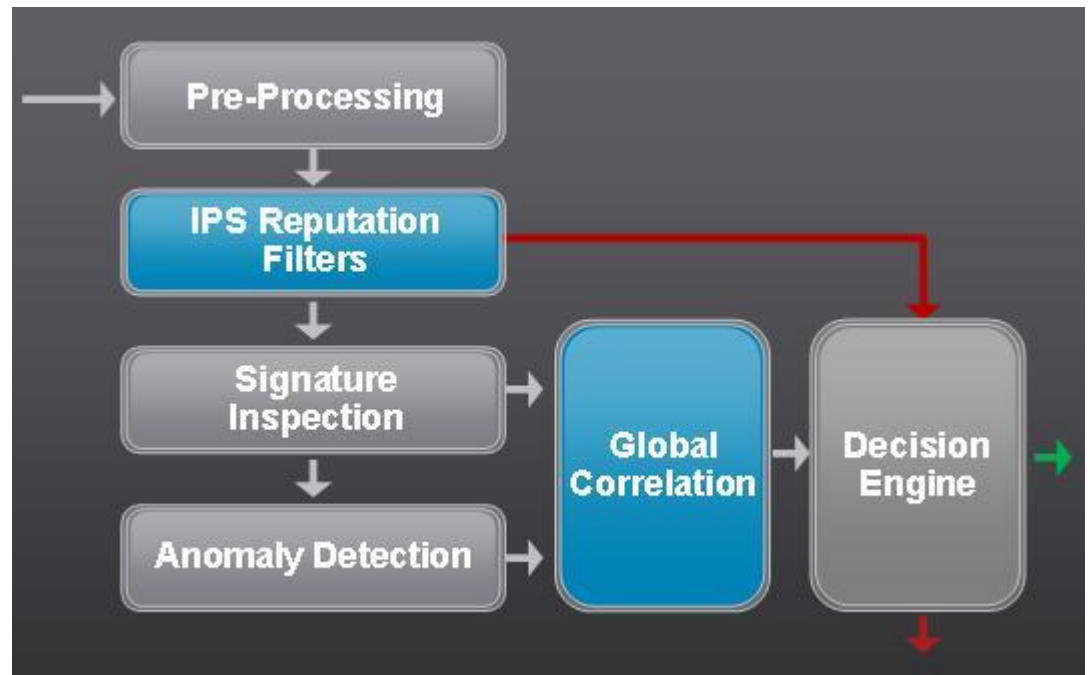
IPS 7.0 with Global Correlation



Charlie Stokes
Technical Marketing Engineer

Packet Flow in IPS v7.0

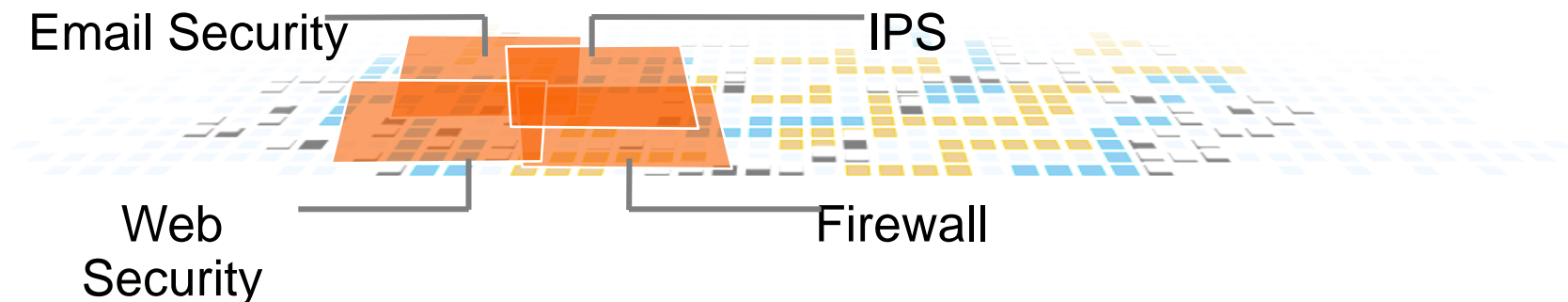
- IPS Reputation Filters block access to IP's on stolen 'zombie' networks or networks controlled entirely by malicious organizations.



- Global Correlation Inspection raises the Risk Rating of events when the attacker has a negative reputation allowing those events to be blocked more confidently and more often than an event without negative reputation.

What is Reputation?

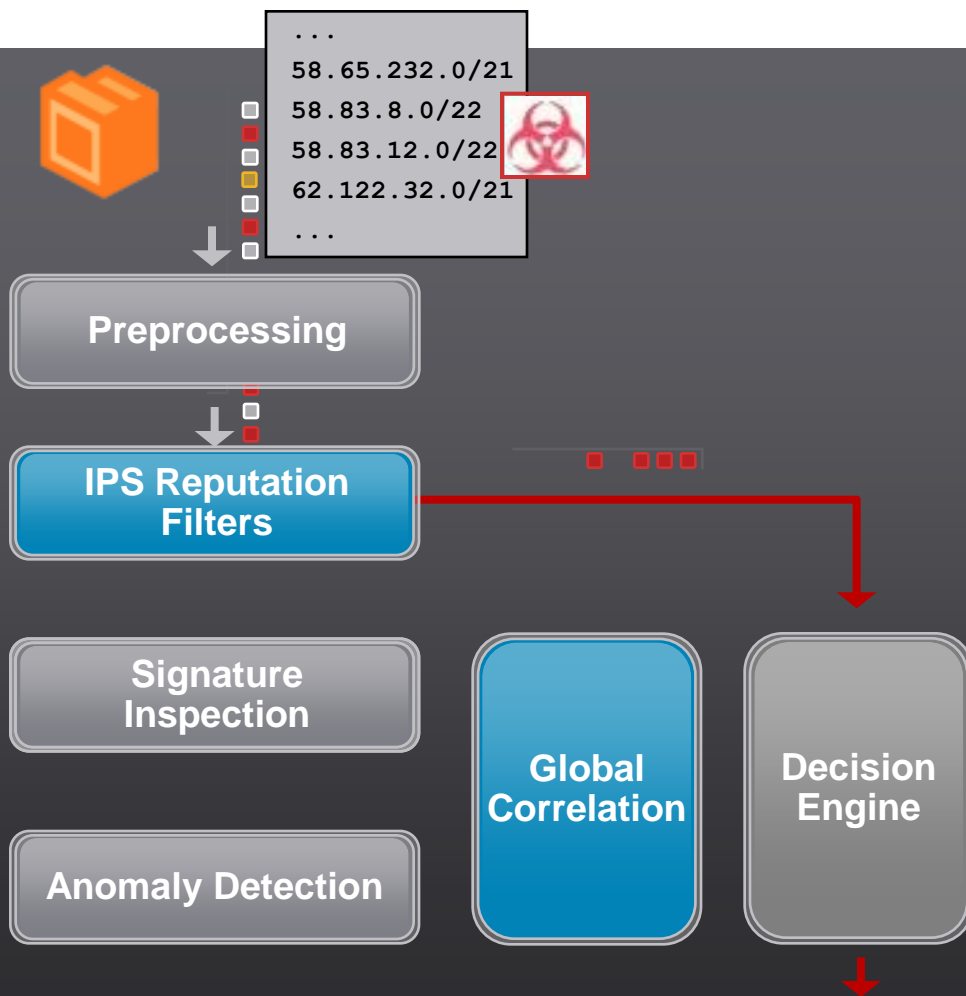
or “Is all reputation the same?”



- Reputation is the history of both actions and qualities of a specific IP address or network. This is calculated using some of the hundreds of different types of data found in Sensorbase.
- For different types of devices, different parameters can mean more or less for the reputation of a device.

Ex: The fact of sending SPAM is highly relevant to an email reputation device and less so to an IPS sensor.

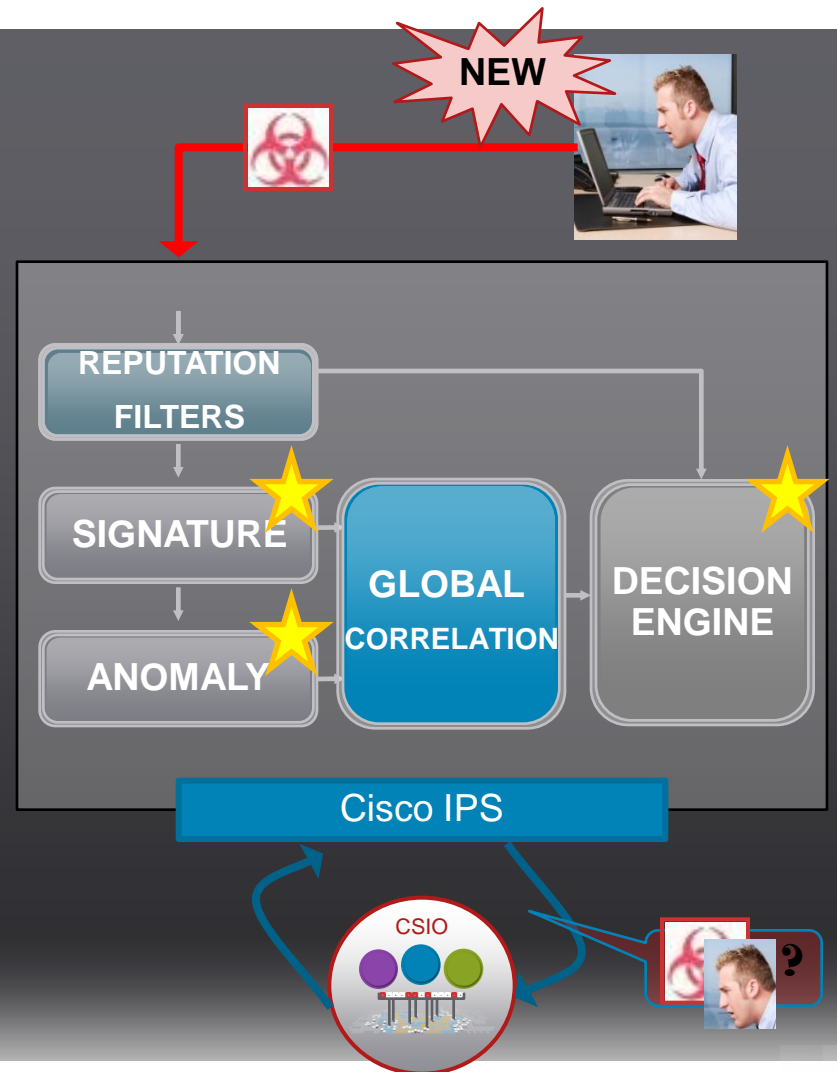
IPS Reputation Filters: Blocking the worst bad apples



- Some networks on the Internet are owned wholly by malicious organizations or are hijacked 'zombie' networks
- Reputation Filters block access to these networks like an ACL
- Individual IP addresses do not go on this list because of things they do (An IP does not go from -1 to -9 to being put on this list)

Local Inspection will Always Matter

Example 1: Unknown Attacker

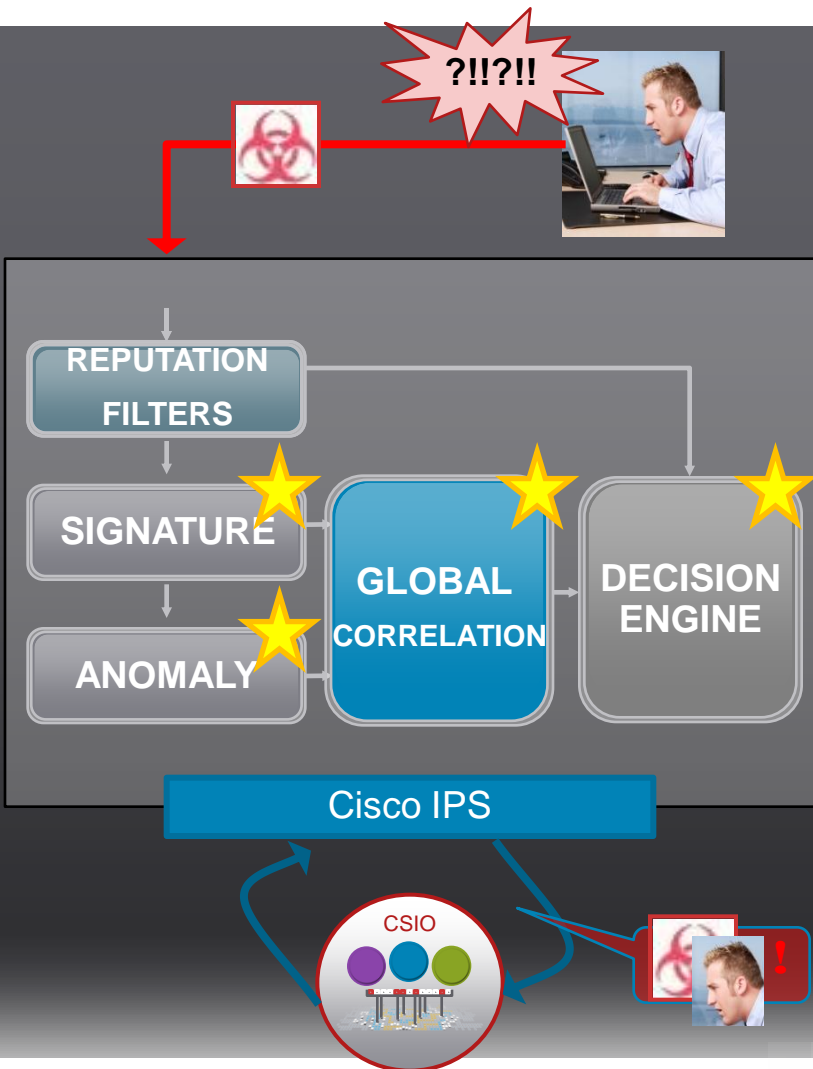


1. New Attacker hits the IPS
2. Attacker without a Reputation
3. Signatures or Anomaly Detection identify activity
4. The attack is handled according to the security policy implemented on the sensor (Deny if Risk Rating reaches threshold)
5. Information on the Attacker is sent back to CSIO to track his reputation (if configured)

Global Correlation Inspection

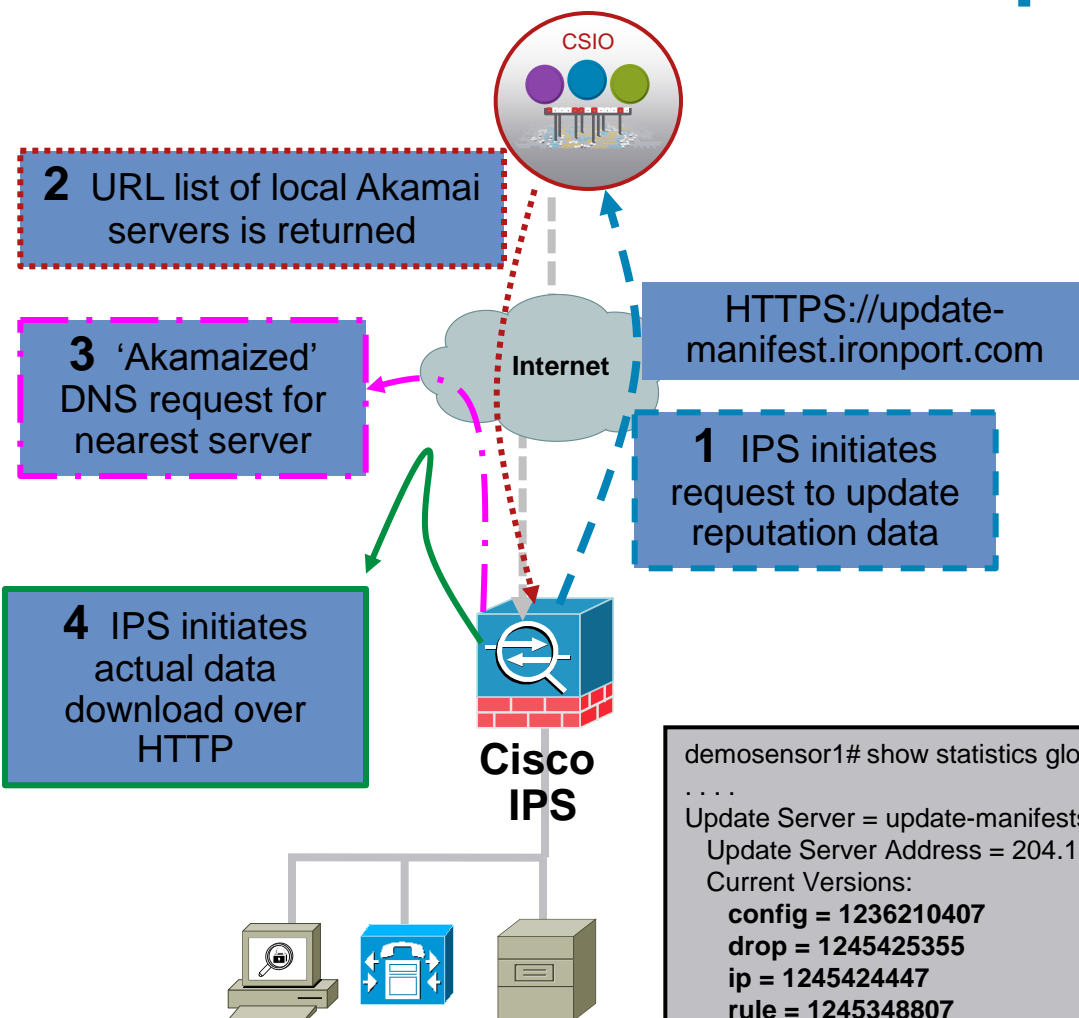
Example 2: Suspicious Attacker

Identified through Local Inspection, Denied due to Global Correlation



1. Suspicious Attacker attacks
2. Has medium Reputation
3. Signatures identify suspicious activity and give this a medium Risk Rating
4. Global Correlation adds context of Attacker Reputation to Risk Rating
5. Decision Engine blocks
6. Information on NEW Reputation is sent back to CSIO.

Global Correlation Reputation Updates

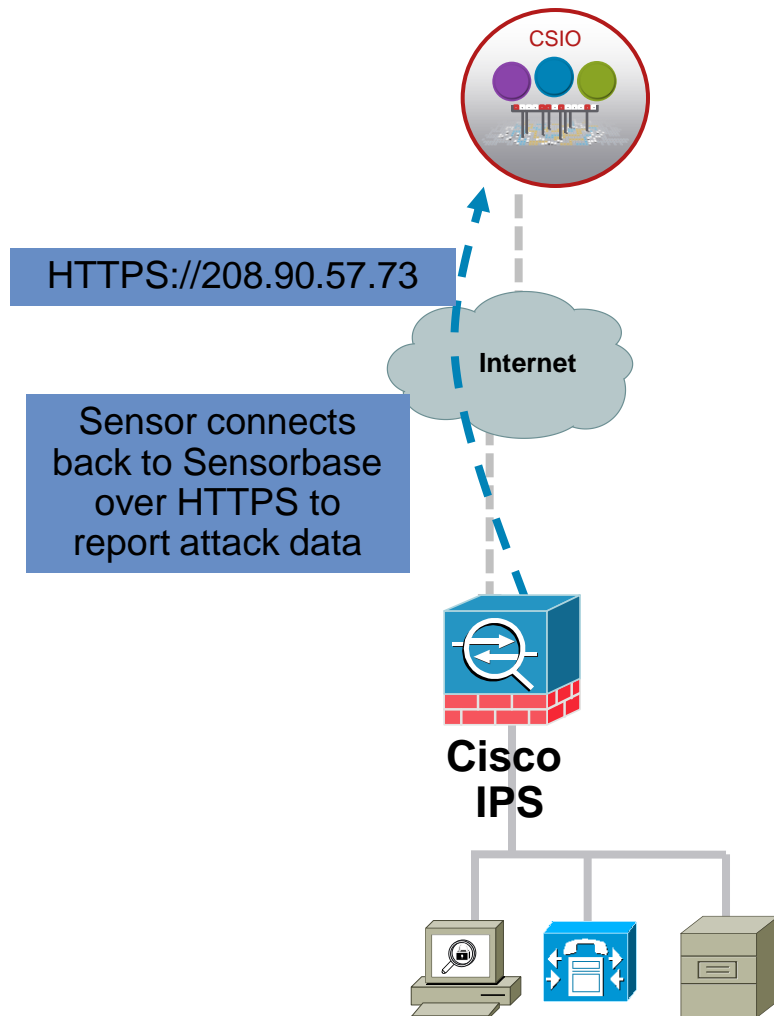


1. Initiate request to update reputation data through HTTPS request
2. Sensor gets back a manifest containing the DNS name of a server to get the data from
3. DNS request returns the nearest Akamai server
4. Initiate actual data download using HTTP from the Akamai server

```
demosensor1# show statistics global
....
Update Server = update-manifests.ironport.com
Update Server Address = 204.15.82.17
Current Versions:
  config = 1236210407
  drop = 1245425355
  ip = 1245424447
  rule = 1245348807
```

Reputation data comes in the form of multiple files (config, drop, ip, rule) that get downloaded as needed during updates

Global Correlation Network Participation: or “My sensor is sending data back to Cisco?”



- Event data parsed down into Reputation update data on the sensor and buffered for transmission to Cisco Sensorbase
- Every ten minutes on average, network participation data is sent to Cisco over HTTPS
- This data does not include private addresses
- Network Participation improves overall security as well as your own by feeding in attackers data specific to your site.

Global Correlation Network Participation: or “What is my sensor sending back to Cisco?”

Network Participation

Select the extent to which the sensor will contribute data to the SensorBase network.

- ☒ Off Do not contribute data to the SensorBase network.
- ☐ Partial Contribute data to the SensorBase network but withhold some potentially sensitive information.
- ☐ Full Contribute all alert data to the SensorBase network.

Network Participation Disclaimer

If you agree to participate in the SensorBase Network, Cisco will collect aggregated statistics about traffic sent to your IPS. This includes summary data on the Cisco IPS network traffic properties and how this traffic was handled by the Cisco appliances. We do not collect the data content of traffic or other confidential business or personal information. All data is aggregated and sent via secure HTTP to the Cisco SensorBase Network servers in periodic intervals. All data shared with Cisco will be anonymous and treated as strictly confidential.

The table below describes how the data will be used by Cisco.

Participation Level	Type of Data	Purpose
Partial	Protocol Attributes (e.g. TCP max, segment size and options string)	Track potential threats and understand threat exposure
	Attack Type (e.g. Signature Fired and Risk Rating)	Used to understand current attacks and attack severity
	Connecting IP Address and port	Identifies attack source
	Summary IPS performance (CPU utilization memory usage, inline vs. promiscuous, etc)	Tracks product efficacy
Full	Victim IP address and port	Detect threat behavioral patterns

Agree

Disagree

- Network Participation is entirely voluntary and on an Opt-In basis (off by default)
- No actual packet content data is ever sent back
- Partial participation sends back Attacker IP, port, Sig ID and Risk Rating, some protocol attributes and summary IPS performance data
- Full mode adds in Victim IP and port
- Private IP addresses are removed before sending

Q and A



